スマホとサイバー戦争――戦争の加害者にも被害者にもならないために

JCA-NET セミナー
2026/4/22
Toshimaru toshi@jca.apc.org

本日のセミナーのテーマ

- ウクライナへのロシアの侵略戦争からガザでのイスラエルによるジェノサイド、そして現在進行中の米国とイスラエルによるイランへの戦争に至るまで、サイバー領域は、否応なしに実空間での戦争遂行にとって不可欠な手段になっています。
- サイバー領域のなかでも、私たちに身近なスマホやパソコンが戦争に果す役割もまた無視できないものになっています。戦場の兵士のスマホなど通信機器は、軍が運用する AI を駆使した攻撃システムと連動して武器として機能します。他方で戦場の非戦闘員である市民たちは、自身のスマホで戦争とその被害を記録し、SNS などを通じて多くの人たちに拡散することができます。
- こうした SNS などでの情報発信は、戦争のプロパガンダにも反戦運動にも用いられますが、同時にヘイトスピーチや偽情報の拡散の手段にもなります。そして、SNS を運用する大手通信事業者は、メッセージを自由に検閲したり遮断する力をもち、戦争犯罪の重要な証拠となるデータを削除する力も持ちます。こうした通信事業者と政府が連携したときには、いったいどのようなことが起きるでしょうか。私たちは、スマホやパソコンを通じて否応なしに戦争の当事者にならざるをえない状況にあります。今回のセミナーではこのスマホやパソコンという私たちの生活必需品の「武器化」の問題を考えてみます。

何を問題にしたいのか

- 戦場は私たちの向こう側だけでなく、私たちの掌のなかにある。
- 私たちは、スマホを通じて戦争の当事者になりうるし、そうなるように政府もスマホを戦争体制に組み込もうとする。
- 「私は戦争に反対だ」という自分の意思に反して、スマホやパソコンを使うことを通じて戦争への加担者になりうる。
- 私たちの通信情報は、どのように些細なものであれ、戦争にとって有益な材料になりうる。
- 私たちの SNS での「いいね」が戦争の扇動や戦意高揚、あるいはヘイトスピーチのプロパガンダになりうる。

概要

- スマホと戦争について現在どのような議論があるのか
- (紹介)Matthew Ford, War in the Smartphone Age
- スマホと私たちの日常
- ウクライナ戦争の場合： SNS
- ウクライナ戦争の場合：ウクライナ IT 軍
- ウクライナ戦争の場合：参加型戦争
- ウクライナ戦争の場合：ファクトチェック
- 戦争の読まれ方： SNS を通じた戦場
- ウクライナ戦争における官民連携
- これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

参考文献

参考文献

Matthew Ford, War in the Smartphone Age, C. Hurst & Co. (Publishers) Ltd., 2025

https://www.hurstpublishers.com/book/war-in-the-smartphone-age/

Jack McDonald, Digital Connectivity and Digital Informants in War

https://carnegieendowment.org/research/2025/07/digital-connectivity-and-digital-informants-in-war

Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?

https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/

(国際赤十字委員会) 武力紛争下におけるデジタル脅威からの民間人の保護

https://shop.icrc.org/download/ebook?sku=4735.01/002-ebook

(国際赤十字委員会) 国際人道法と、武力紛争下におけるサイバー作戦およびその他のデジタル活動への民間人の関与の拡大

https://www.icrc.org/sites/default/files/2025-11/4895_002_IHL_and_Civilian_Involvement_in_Cyber_Op_WEB.pdf

スマホと戦争について現在どのような議論があるのか

(lieber.westpoint.edu) ウクライナ・シンポジウム——携帯電話で通報する民間人は、敵対行為に直接加担しているのか？

著者：マイケル・ N ・シュミット、ウィリアム・ケイシー・ビガースタッフ | 2022 年 11 月 2 日

マイケル・ N ・シュミット：ウェストポイントの米国陸軍士官学校における G ・ノーマン・リーバー特別研究員。レディング大学の国際公法教授、米国海軍戦争大学の名誉教授兼チャールズ・ H ・ストックトン特別客員研究員、およびテキサス大学のストラウス・センター特別研究員兼法学客員教授。

ウィリアム・ C ・ビガースタッフ少佐：米国海軍戦争大学ストックトン国際法センターの軍事教授、同センターで武力紛争法の講義を共同担当。

ロシアが空から電力網やその他の重要インフラへの激しい攻撃を続ける中、ウクライナは自国の空を守るための方法を創意工夫して開発している。その新たな手段の一つが「 ePPO 」だ。これは**ウクライナの民間人が携帯電話にダウンロードし、飛来するミサイルやその他の航空脅威の位置を報告できる新しいモバイルアプリケーション（「アプリ」）**である。

スマホと戦争について現在どのような議論があるのか

ウクライナ・シンポジウム——携帯電話で報告する民間人は、敵対行為に直接加担しているのか？ (続)

例えば、報道によると、10 月 22 日には、ウクライナ軍がこのアプリのデータを活用し、移動式防空システムを用いてカリブル巡航ミサイルの撃墜に成功した。こうした巡航ミサイルや爆発物を搭載した無人航空機は、ロシアが重要インフラを標的とするための主要な兵器の一つである。

このアプリの使用は、

- **敵の脅威を通報するためにアプリをダウンロードして使用するウクライナの民間人が、「敵対行為に直接参加している」のか、したがって国際人道法 (IHL) の下でロシア軍による攻撃対象となり得るのか**
- **攻撃対象になる場合は、いつどのような状況でなのか**

スマホと戦争について現在どのような議論があるのか

「戦争におけるデジタル接続性とデジタル情報提供者」

ジャック・マクドナルド著 2025 年 7 月 31 日

ジャック・マクドナルドは、キングス・カレッジ・ロンドンの戦争研究学部で上級講師。同大学の科学・安全保障研究センターの所長も兼任。戦争の規制や、技術革新によって生じる倫理的問題を研究

https://carnegieendowment.org/research/2025/07/digital-connectivity-and-digital-informants-in-war

デジタル通信技術、特にスマートフォンは、紛争地域における民間情報提供者の力を増大させた。**軍隊は歴史的に、民間人がスパイとして活動したり、敵対する武装勢力に情報を提供したりする可能性があるという事実に対処**せざるを得なかった。しかし、**今日の武力紛争を目撃する民間人は、写真や動画、さらには GPS 位置情報をほぼ瞬時に送信できるスマートフォンを持っている**ことがほとんどだ。この情報は、現地レベルでは、こうした民間人の情報を基に敵軍への直接攻撃を可能にし、作戦レベルでは、軍の配置や動静をより深く把握することを可能にする。

スマホと戦争について現在どのような議論があるのか

「戦争におけるデジタル接続性とデジタル情報提供者」(続)

敵味方双方の交戦当事者が注視するソーシャルメディアに写真を撮り投稿するといった比較的些細な行為でさえ、重大な結果をもたらし得る。 … 今日のデジタル紛争の観察者は、信頼性が高く、タイムリーで、豊富かつ正確なデータを送信でき、その**データは本質的に軍事判断やキルチェーン [殺害行為に結果するまでの一連の流れ] に統合可能である。戦闘員は、観察者の軍事装備に関する知識 … に依存することなく、撮影された装甲戦闘車両の型式を [画像データベースなどで] 確認できる。同様に、写真や動画データは、口頭でのコミュニケーションでは捉えられない正確な地理位置情報を提供できる。**

その結果、デジタル接続性は戦争への参加という概念を揺るがしている。**現代の紛争におけるデジタル観察者や情報提供者が果たしている性格、あるいは彼らが戦闘員に及ぼし得る脅威に照らしたとき、戦争における民間人の加害責任に関する法や道徳についての従来の理解と抵触することになりうる。**

スマホと戦争について現在どのような議論があるのか

間諜

間諜の定義

間　諜

第二十九條

交戰者ノ作戰地帶内ニ於テ對手交戰者ニ通報スルノ意思ヲ以テ穩密ニ又ハ虛僞ノ口實ノ下ニ行動シテ情報ヲ蒐集シ又ハ蒐集セムトスル者ニ非サレハ之ヲ間諜ト認ムルコトヲ得ス

故ニ變裝セサル軍人ニシテ情報ヲ蒐集セムカ爲敵軍ノ作戰地帶内ニ進入シタル者ハ之ヲ間諜ト認メス又軍人タルト否トヲ問ハス自國軍又ハ敵軍ニ宛テタル通信ヲ傳達スルノ任務ヲ公然執行スル者モ亦之ヲ間諜ト認メス通信ヲ傳達スル爲及總テ軍又ハ地方ノ各部間ノ聯絡ヲ通スル爲輕氣球ニテ派遣セラレタルモノ亦同シ

参考：スパイとは (ハーグ陸戦条約 1907)

第二章 間諜

第 29 条 : 交戦者の作戦地域内において、敵勢力に通諜する意志をもって、隠密に、または虚偽の申告の下に行動して、情報の蒐集をしようとする者を間諜とする。故に、変装せずに、軍人として情報収集の為、敵軍の作戦地域内に侵入した者は間諜と認めない。軍人であるか否かに係わらず、自軍または敵軍宛の通信を伝達する任務を公然と執行する者も間諜と認めない。

https://ja.wikipedia.org/wiki/ハーグ陸戦条約

スマホと戦争について現在どのような議論があるのか

(国際赤十字委員会) 武力紛争下におけるデジタル脅威からの民間人の保護

民間人が武力紛争に関連するデジタル作戦に参加すればするほど、誰が民間人で誰が戦闘員であるかを区別することが困難になることを認識すべきである。実際には、これは武力紛争中に民間人や民間インフラが標的とされるリスクが高まっていることを意味する。

勧告 5 :交戦当事者は、デジタル作戦を通じて民間人が敵対行為に直接参加することを奨励してはならない。交戦当事者は、民間人に武力紛争に関連するデジタル作戦への参加を奨励した場合、民間人が法的保護を失い、標的とされるリスクがあることを考慮しなければならない。

スマホと戦争について現在どのような議論があるのか

(国際赤十字委員会) 武力紛争のデジタル化に関する共同イニシアティブの研究・専門家協議プロジェクト報告書「国際人道法と、武力紛争下におけるサイバー作戦およびその他のデジタル活動への民間人の関与の拡大」

世界と戦争のあり方が急速にデジタル化される中、武力紛争への民間人の関与は新たな形態をとり、**民間人にとってより容易になり、関連するリスクも新たな規模に達する可能性**がある。実際、近年のいくつかの武力紛争では、**政府が提供するアプリを通じて、民間人が大規模に軍事関連情報を収集するよう奨励**されたり、前例のない数の**民間ハッカー集団**（しばしば「ハクティビスト」と呼ばれる）が、自らが敵とみなす対象に対してサイバー作戦を実施したり、**テクノロジー企業が、自社の資産、従業員、顧客に対するリスクに気づかないまま、交戦当事者にサービスやインフラを提供**したりする事例が見られる。この傾向は、武力紛争下における民間人の安全に深刻な影響を及ぼしている。

スマホと戦争について現在どのような議論があるのか

たとえば、侵略戦争の加害国ロシアの多数の人びとが侵略戦争を否定していない、イスラエルの圧倒的多数の人びとはガザや西岸での軍事行動を支持している。ウクライナ、ロシア、イスラエルの兵役拒否者の抗議の声の存在がほとんどメディアからも SNS 上からも目立たない状況に追いやられている。たぶん、日本も同じ道を歩む可能性が高い。この状況は、戦争を肯定する権力が構築してきたものだ。

スパイ機関創設関連の法・制度整備がもたらす広がりは、プライバシーの権利や言論・表現の自由の権利への深刻な侵害にとどまらない。むしろ、この法・制度整備は、こうした権利自身を市民自らが自発的に放棄し、国家意思に同調するようなライフスタイルへと切り替えを行なわせるための、地均しになるだろう。

Matthew Ford, War in the Smartphone Age

マシュー・フォード

スウェーデン国防大学戦争学准教授

著書

『 War in the Smartphone Age 』

『 Weapon of Choice 』

共著

『 Radical War 』

『 British Journal for Military History 』の創刊編集長を務めた。
専門は、技術と戦争。



Matthew Ford, War in the Smartphone Age



反戦や平和を主張する研究者ではなく、むしろ「国防」の観点に立つ研究者。本書が主に参照しているウクライナとガザの戦争についての理解は私とは根本的に異なるところがある。

しかし、日本政府が進めようとしているサイバー攻撃・サイバースパイの問題を考える上で、本書の記述は、すでに起きている戦争を素材として、実際に行なわれている政府、軍、民間企業の行動を紹介している点で参考になる。

自分たちが利用しているスマホがどのようにして戦争に組み込まれ、私たち自身がどのように戦争に加担してしまうことになるのかを知ることは、日本政府の戦争を阻止し、戦争に加担しないライフスタイルを構築するにはどうしたらいいかを考える上で、参考になる。

Matthew Ford, War in the Smartphone Age

目次

第一部 指先の危機

- 歪んだ戦争
- 戦争を解読する

第二部 二つの形成戦争 (shaping war)

※大規模な戦争を開始する前の準備段階として、有利な状況を形成する (shaping) ための戦争。一般に shaping operation という。

- スタック
- キルチェーン

第三部 戦場の (新たな) 様相

- 参加戦争行為
- 加速化される戦争

スマホと私たちの日常

スマホひとつあれば、私たちは出来事を記録したり、仕事や恋人を探したり、地球の反対側に住む友人と会話したり、政治家やスターに疑問を投げかけたり、スタッフを管理したり、自分の位置を確認したり、道順を調べたり、体験をソーシャルメディアに投稿したり、住宅ローンを申し込んだり、新聞を読んだり、リアリティ番組を観たり、タクシーを呼んだり、ゲームをしたり、別荘を借りたり、ほぼ何でも購入でき、明日には別の国に住む友人の玄関先に荷物を届けてもらうこともできる。**しかし、決定的なこととして、 2024 年現在、スマートフォンは戦争の主要な兵器としても使用されているということだ。**兵士たちは、最新の TikTok ダンスやユーロビジョンの動画の類いをシェアするのと同じくらい簡単に、**手のひらサイズの小さなデバイスを使って、武装したドローンを標的に誘導したり、戦場の残虐行為をネット配信したり、あるいは自身の位置情報を漏らしたりすることができる**のだ。 (Matthew Ford)

スマホと私たちの戦争

「民間人は今や、スマートフォン一つで情報の作成、発信、消費ができる。これが**戦争への参加**のあり方を変えた」

民間人は、軍が敵を発見・捕捉・殺害するのと同じように、こうしたことを行える⇒**一般市民は戦闘において直接的な役割を果たせるようになる。**

「これにより、スマートフォンとその利用者はキルチェーンの一要素となり、標的に対して兵器を投入するプロセスが短縮される。」

戦場の様相が変わる。「今や、軍人であるか否かを問わず、誰もが情報収集や標的指定の参加者となり得る。 ... 暴力の政治に劇的な影響を及ぼしている。」

ウクライナ戦争の場合： SNS

「ウクライナ戦争が始まると、ソーシャルメディアは活気づいた。 YouTube のゲーマーチャンネルは侵略に関する分析をライブ配信し、ロシア軍の進撃ルート沿いの町のウクライナの Facebook グループは、コミュニティに対して侵略者の位置を警告し始めた。誰もが突然、戦争の専門家になったのだ。 ...(Google Map では) 突然、ライブの交通マップでロシア軍の戦車部隊を特定できるようになり、ソーシャルメディアユーザーは主流の放送メディアに頼ることなく事態の展開を見守ることができた。 Google Maps はウクライナ人に避けるべき道路を教える一方で、ウクライナ軍は砲兵や対戦車部隊をどこに集中させるべきかをこれで知った。ストリートカメラの位置を知り遠隔でアクセスできれば、それをソーシャルメディアで配信し、世界中の誰もがロシアの装甲部隊が高速道路をゆっくりと進む様子を見られるようにできた。人々は新しい映像を求めてウェブをくまなく探し回り、主流メディアのジャーナリストたちより先にスクープを狙った。その見返りは、ウクライナで進行中の危機について何かを知ることだけにとどまらず、未公開の映像を公開することでフォロワー数が増加したことにもあった。」

⇒こうした映像が、時系列も含めて全て真実かどうかの判断にファクトチェックは欠かせないがソーシャルメディアの発信者は信憑性よりも速報性に惹かれて発信する。既存メディアもソーシャルメディアに発信の遅れをとりたくないため、ファクトチェエクが甘くなる。

ウクライナ戦争の場合：ウクライナ IT 軍

- ウクライナのサイバー技術起業家エゴール・アウシェフが主導、 2022 年 2 月 24 日に結成された。正式のウクライナ軍の組織ではないが、政府が全面的にバックアップ。
- IT 軍は、世界中の才能ある人材を動員し、世界各地の個人を巻き込む。

- 誰もが戦争に容易に参加できる体制⇒「戦争参加の民主化」：テクノロジーと市民参加が密接な関連性をもちながら国家安全保障に関わる。
- 他方で、ウクライナ以外の国からの IT 軍の参加者は、戦闘員なのかどうか、参加することについての各国の国内法上の問題はないのかどうか、などの問題が提起される。

在日ウクライナ大使館、志願兵募集の投稿　元自衛隊員ら約70人応募

2022年3月1日 23時12分

list　26



在日ウクライナ大使館のツイッター

ロシアのウクライナ侵攻を受け、在日ウクライナ大使館が志願兵を募ると公式ツイッターに投稿している。自衛隊などでの経験を条件に挙げる。林芳正外相は1日午後の閣議後会見で、投稿を把握しているとしたうえで「ウクライナ全土に退避勧告を発しており、目的を問わず同国への渡航をやめて頂きたい」と述べた。

ウクライナ戦争の場合：参加型戦争

- ウクライナ侵略から 3 日後、ロシア軍はベルジャーンスクを占領。ベルジャーンスク占領に対するウクライナの反撃は 5 日後に発生。この間、 SNS 上に、現地市民、ロシア側メディアなど多くの動画などが投稿される。
- 当局による取り締まりが始まる前にすでに人々は自由に戦争の映像を配信。
- 軍事通信インフラと民間通信インフラが並行して機能し続ける。
- ウェブカメラの映像は、ロシア艦船が港に入港する様子を捉える。
- スマートフォンの映像は、ベルジャーンスクへのロシア軍の進軍経路を可視化し、占領への市民の不満を記録。
- これらはすべて、ロシア人やウクライナ人、そしてソーシャルメディアを通じて配信⇒世界中の人々が目に。

ソーシャルメディアや街中の監視カメラなどのスマートデバイスが普及することによって、軍が一般市民による情報発信を統制できなくなった。これは侵略者側と防衛軍側に共通して生じる新しい戦場の状況である。

ウクライナ戦争の場合：参加型戦争

スマートデバイスの民間主導のセンサーネットワークはダイナミックな標的選定サイクルを生む。

- 情報分析官はあらゆる情報源からの収集と評価を行わなければならない。
  - オンラインや主要メディアを通じて配信された画像
  - 戦場の軍事部隊や民間人から報告された情報

を統合する必要がある。そのためには、

民間人のスマホによる報告の迅速分析⇒砲兵部隊に標的座標伝達⇒民間人から提供される情報の標準化が必要。⇒相当な事前計画と準備が必要

- 敵の動静の記録方法を市民に案内するスマートフォンアプリ、チャットボット（自動応答システム）、およびウェブページの作成
- これらの制作をウクライナの治安機関 SBU が調整し、ウクライナの非営利団体「カム・バック・アライブ財団」がクラウドファンディングで資金調達
- 全面侵略の開始当初、チャットボットと関連ウェブページの存在を Telegram で告知
- 占領軍の位置を報告するためにスマホに搭載できる e-Vorog（ e-Enemy ）アプリが敵の動静を報告。

ウクライナ戦争の場合：参加型戦争

e-Vorog アプリとは

- 情報収集のための標準化されたテンプレート。
- 訓練を受けていない民間人がウクライナ軍に有用な情報を提供するプロセスを簡素化
- 民間人は必要な情報を e-Vorog に入力するだけで、軍のアナリストがデータ処理を行う

⇒民間人は実行可能かつ迅速な方法で、標的選定サイクルに直接貢献できるようになった。

実際、侵略開始から最初の 4 ヶ月間で、 28 万 7,000 人のウクライナ人がロシア軍の動向や装備に関する情報を提供した。

もしその個人が敵陣地内にいた場合、彼らがこのアプリケーションを使用すればスパイ罪で有罪となり、処刑されるリスクにさらされるとウクライナは判断している。

ウクライナ戦争の場合：参加型戦争

e-Vorog 以外にもウクライナの IT セクターによるモバイルデバイス向けのアプリ群が開発された。(民間防衛と市民の動員に用いられるアプリ、ウクライナの偵察・攻撃システムを強化するアプリなど)

例えば、 ePPO アプリ。ウクライナの非営利団体「アエロロズヴィドカ Aerorozvidka 」によって構築・維持され、ボランティアによるクラウドファンディングで資金調達。

一般市民がロシアの航空機、ミサイル、ドローンの目撃情報を報告できるアプリ。スマートデバイスを航空機やドローンに向けてボタンを押すだけで、位置情報を軍に送信する。

市民は迫り来る空襲警報を発する役割を担う。アプリから得られたデータが集約され、スマホ通知を通じて空襲警報を人々に広く配信。

ePPO は、軍事システムによって生成された情報資料と統合され、**ウクライナの状況認識プラットフォーム「デルタ Delta 」**に組み込まれている。

ウクライナ戦争の場合：参加型戦争

スマホアプリの多くは、クラウドファンディングやプライベートな支援で運営

- Army-SOS が開発した指揮統制（ C2 ）プラットフォーム「**クロピヴァ（イラクサ）Kropyva (Nettle)** 」：戦線をマッピングし、砲撃任務を計算する。
- NGO 「ノオスフィア Noosphere 」が支援するメッセージングアプリ「**ミルチャット MilChat** 」：部隊と指揮官間の通信を可能にし、部隊の動きの追跡や資源配分の最適化を支援する。
- 「 **GIS Arta** 」 (2014 年から運用) ：様々な情報源から得た標的情報を砲兵用の正確な座標に変換。 Uber のソフトウェアと同様の機能を備え、ウクライナの IT ボランティアによって開発された。
- Google Play で利用可能な「 **Ukrop/MyGun** 」： UkropSoft によって開発され、地形、気象、弾道情報を考慮して砲兵部隊向けの標的データを算出。

ウクライナ戦争の場合：ファクトチェック

膨大な映像などの記録のファクトチェックをいかにして行なうか。

- 2022 年のロシアの侵略の最初の 80 日間だけで、 10 年分の映像が記録された。
- 膨大な情報の真偽判断の作業 (ファクトチェック) が追いつかない。
- ファクトチェックの重要性に一般市民が高い関心を抱かない。
- 戦争犯罪を裁く司法の判断も追いつかない。

戦争犯罪を裁く上での大前提になる司法上の有効な証拠をどのように判別して残していくか。

戦争の読まれ方： SNS を通じた戦場

バークレープロトコル：国際刑事法、人権法、人道法違反の調査におけるデジタル・オープンソース情報の有効活用に関する実践ガイド (2022/1) カリフォルニア大学バークレー・ロースクール + 国連人権高等弁務官事務所

「国際刑事法、人権法、および人道法に違反したとされる事案についてオンライン調査を行うための国際基準を定めている。」責任を負うべき者を法の下に裁くために必要な証拠のありかたなどを定めようとするもの。

https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source



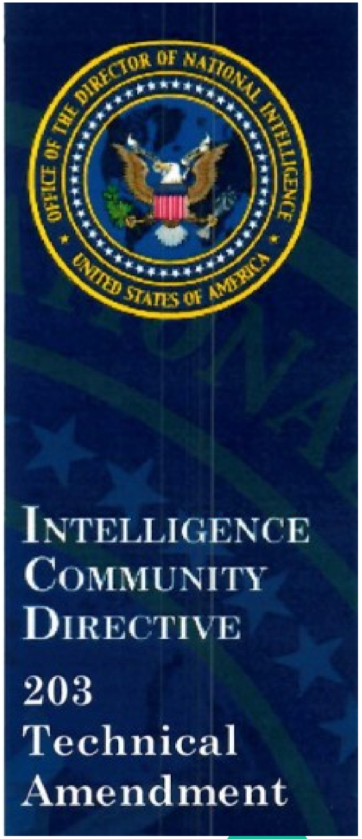
戦争の読まれ方： SNS を通じた戦場

オープンソース・インテリジェンス

諜報機関にとってネット上の公開情報をどのように評価するか (偽情報など様々な不純物が混在する) が新たな問題になった。 ICD203 は、米国の全 18 諜報機関において、何が信頼できる諜報分析とみなされるかを定めた。

https://www.dni.gov/files/documents/ICD/ICD-203.pdf

- 通信網、サーバーセンター、スマートデバイス、衛星通信、検索エンジン、ウェブベースのアプリケーション、ソーシャルメディア企業など、情報インフラの複雑な相互作用
- 他方で軍はそれぞれの情報機関からの特権的な情報



ウクライナ戦争における官民連携
政府データの国外退避

ロシアによる全面侵略の 1 ヶ月前、 AWS はウクライナ政府高官と会談し、同国のデジタル記録を保護するために企業がどのように支援できるかを協議⇒ウクライナの記録と政府の電子サービスをすべてクラウドに移行すること。

ロシアによる全面侵略後の数週間で経済、税制、銀行、政府の電子サービスに関連する機能など政府の主要なデータが国外の AWS のデータセンター内のクラウドに移される。

同時に、 AWS はサイバーセキュリティおよび多数のクラウド提供型サービスやアプリケーションを提供。

「ウクライナの場合、アマゾン・ウェブ・サービス（ AWS ）は現在、クラウド上の安全なサーバーにウクライナ政府のシステムをホストしている。これにより、**たとえ政府機関がロシア軍の進撃によって制圧されたとしても、 AWS はウクライナが国内の市民社会を管理し続ける能力を保証している。」**

「たとえウクライナが領土として消滅したとしても、世界中に散らばるグローバルなディアスポラを擁する仮想空間として存続し続ける」

ウクライナ戦争における官民連携
脅威インテリジェンス

多くの民間企業がウクライナに対しサイバー防衛支援（CDA）や脅威インテリジェンスを提供している。

CDA には、民間セクターによるテクノロジー（ソフトウェアライセンスやサイバーセキュリティツール）の提供、データ分析支援、脅威インテリジェンス・プラットフォームへのアクセス、およびサイバーセキュリティ・コンサルティングが含まれる。

ウクライナの場合は CDAC という民間企業による連合体が結成されている。 Microsoft や Google などの企業で構成される CDAC は、民間セクターによるウクライナへの関与を調整

https://crdfglobal-cdac.org/



ウクライナ戦争における官民連携
戦時検閲

ウクライナ侵略の一環として、ロシアはウクライナの人々と欧州の人々を標的とした誤情報キャンペーンを展開した。

Meta 、X 、YouTube といった主要なソーシャルメディア企業は、こうしたロシアの軍事作戦を制限するための措置を講じた。

- Meta の場合、ウクライナ戦争に関するコンテンツの管理に特化した特別対策センターの設立。その結果、Meta は RT などのロシア国営メディアがウクライナや欧州で配信することを遮断し、これらのアカウントをロシアメディアとして明示し、投稿の事実確認を行い、禁止されていない場合でもコンテンツの収益化能力を制限した。
- Google の場合。YouTube 上のロシア国営メディアのアカウントを遮断し、ロシアの団体による Google Ads の利用を阻止し、ロシア政府系情報源からの検索結果の優先順位を下げた。

ウクライナ戦争における官民連携
戦時検閲

「ウクライナ侵略を受けて、Facebook はロシア人に対する政治的暴力を表現する投稿を許可する用意があり、「通常であれば当社のルールに違反するであろう政治的表現の形態について、一時的に容認している」と述べている。」

ロシアに対して実施されたプラットフォーマーによるソーシャルネットワークによる様々な検閲は規制措置が、ガザへのイスラエルのジェノサイドでは、ガザ、パレスチナ人に対して行使された。

民間プラットフォーマーのこうした力のありかたを私たちはどのように判断すべきなのか。⇒プラットフォーマーに依存しない言論空間の構築が必要。その際に私たちは、営利目的や国策、ナショナリズムによって支配されるのではない言論空間の構築を目指す、という明確な目標をもつ必要がある。

これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

「スマートフォンは情報収集の範囲を軍から市民社会へと拡大させた一方で、テクノロジーによって民間人と戦闘員の境界線を曖昧なものにしてしまったのである。ロシア兵は、個人をどう扱うかを決める前に、民間人の携帯電話を確認することになる。現実には、こうしたアプリの存在自体が、今やすべての民間人をリスクにさらしている。 ... 単にスマートフォンを所持しているという事実だけで——武力紛争法の解釈がどうであれ——たとえそのデバイスを使って敵を撮影していなくても、民間人はスパイや戦闘員とみなされることになる。」

「スマートフォンがいかに戦闘の様相を変えているかが改めてわかる。そこで問題となるのは、戦場の境界をどのように定義するかだ。 ... 中立国の民間人であっても、前線のウクライナの民間人と同様に、ウクライナの統合情報分析チームに標的情報を提供することができる。標的選定はまた、ウクライナ軍と共にオープンソース情報を分析する民間企業にも委託されている。 この複雑な社会技術システムの網は、攻撃対象領域を拡大させる。これらの個人や組織、さらにはデータセンター、衛星、携帯電話網、海底ケーブルが正当な標的かどうかという問題が生じる。」(Ford)

これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

高市政権による政府のスパイ活動を法的制度的に強化しようとする政策とは ...

- 一般市民が保有する情報を政府が国家安全保障に利用できるようにする。そのための技術的・制度的な枠組を構築する。
- 政府が保有している既存のデータを統合し民間のデータも含めて自由に利用する。
- スマホなどによるリアルタイム情報を政府に自発的に提供できる体制の構築。アプリ開発や SNS を通じた政府との連携の習慣を構築する。
- これらを国家安全保障や治安・軍事活動に統合するためのインフラとシステム構築。
- 膨大なデータの収集と処理⇒民間企業 (外国企業を含む) との連携。

法案の成立のいかんに関わらず、こうした方向をとることは間違いない。

これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

政府にとっての最大の問題は、一般の市民が保有するスマホなどをいかにして情報収集の手段として国策に協力させるか、にある。

- 政府への自発的な協力を可能にする枠組構築
- 政府の枠組にとらわれない市民の自発的な戦争協力の組織化

これらを通じて、プライバシーの権利や言論・表現の自由の権利を自発的に放棄させることを政府は画策するだろう。⇒国家安全保障は、プライバシーの権利や人びとの人権保障の枠外にある例外領域であるということを人びとの「常識」にして浸透させることを狙う。

政府の安全保障政策は、イデオロギーの面からみたときには、「日本」「日本人」を守る、という体裁をとる。(実際には現政権の権力の維持という政治的な欲望がその根源にあるが、これが表にはでないような言説によって、カモフラージュされる)⇒ ナショナリズムによる心情的な同調圧力⇒社会的マイノリティの排除

これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

つまり ...

高市政権は、あらゆる情報を網羅的に収集することを否定していない。この網羅的な情報収集のためには、IT 関連企業を中心とした官民連携とともに、スマホやパソコンという情報端末を保有する私たちについても、情報収集のシステムに組み込み、その情報をリアルタイムで網羅的に収集できる体制をとることが必須である、と判断しているのではないか。

この判断の前提にあるのが、現在世界各地で実際に行なわている戦争における、スマホなど、一般市民が保有する情報端末が果している役割だ。政府は、現在の戦争を見据えながら、いかにして市民を戦争に動員し、市民を情報収集 (スパイ活動) に組み込むかということを考えていることは間違いない。こうした現代の総動員体制を念頭に置いてスパイ機関創設関連の立法化に対する批判を組み立てることが必要だ。

これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

本日紹介した文献でも、スマホが武器になる戦争状況は、民間人をより容易に戦争に巻き込み、戦争は伝統的な文民統制や軍の厳格な指揮命令系統では制御できなくなりつつあることが指摘されている。スマホのアプリの動向をみると、戦争へと向う社会では、ボランティアベースのものも含めて戦争に加担するアプリ開発が加速することがわかる。アイコンをタップする程度のアプリを利用して、人びとが率先して戦争における殺傷行為の一翼を担い、戦争に協力し、戦争を煽る宣伝に加担する仕組みが次々に開発される。こうしたシステムやソフトの開発を押し止める対抗的な動きがほとんどどこにもみられない。また、こうした軍事転用可能なアプリとスマホを手にし、ナショナリズムや正義感に鼓舞された市民が戦争に参加 = 動員する態勢は、戦争を長期化させる要因になりかねない。

私たちが政府のスパイ活動の被害者になるという観点だけでは、十分な批判にはならない。むしろ私たちもまたスパイとしての役割を担わされることになる、ということをより一層自覚する必要がある。

これまでのスパイ機関創設法批判の議論で十分に議論されていない論点

戦争当事国は、侵略した側の国であっても、自国の軍事行動を正当とみなして支持する声が多数を占める。どの国も、自国の戦争を正義のための戦争、自衛の戦争とみなして、人びとを動員する。日本もまた、加害の歴史をもちながら、これを直視せず否定する世論が有力であることを踏まえれば、政府の戦争への動員に抗うことは容易ではない。この動員の構図に抗えなければ戦争を止めることはできないと思う。

誰もが情報発信できるインターネットの環境のなかで、私たちは、今一度、情報発信の力をどのように、何のために、誰のために活用するべきなのかを皆で再確認する必要があるだろう。政治や社会の状況が悪化するなかで、沈黙すべきではないし、持てる発信力を可能な限り生かすことが大切だが、これが政府の監視システムのなかに取り込まれないような工夫——政府には情報は渡さないが、情報を共有する仲間を拡げる——を考えることも大切になる。だからこそ、戦争への動員の「熱」をクールダウンさせ、戦争への動員を押し止め、安全保障の壁で秘匿される国家の情報を開示させるようなアプリやシステム開発、情報発信の環境を構築することが必要だろう。

次回は
4月27日(月)19時から フォローアップ
もしよろしければ
Digital RightsのMLにも登録を